UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/820,790	04/09/2004	Samir Gurunath Kelekar	Q75131	8715

7590 12/20/2007

SAMIR GURUNATH KELEKAR
7/3 EASHWAR JYOTI
KRISHNA REDDY COLONY, DOMLUR LAYOUT
DOMLUR
BANGALORE, KARNATAKA, 580071
INDIA

EXAMINER	
GELAGAY, SHEWAYE	
ART UNIT	**PAPER NUMBER**
2137	

MAIL DATE	DELIVERY MODE
12/20/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/820,790	KELEKAR, SAMIR GURUNATH	
	Examiner	Art Unit	
	Shewaye Gelagay	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 September 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-38* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *9/24/07*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to Applicant's amendment filed on September 24, 2007. Claims 5-38 have been amended. Claims 1-38 are pending.

Response to Arguments

2. Applicant's arguments filed on September 24, 2007 have been considered but are moot in view of the new ground(s) of rejection.

Drawing

3. In view of the amendment filed September 24, 2007, the Examiner withdraws the objection to the drawing.

Specification

4. In view of the amendment filed September 24, 2007, the Examiner withdraws the objection to the specification.

Claim Objections

5. In view of the amendment filed September 24, 2007, the Examiner withdraws the objection to claims 5-14, 17-28 and 31-38.

Claim Rejections - 35 USC § 112

6. In view of the amendment filed September 24, 2007, the Examiner withdraws the rejection of claims 15-28 under 35 U.S.C. 112.

Claim Rejections - 35 USC § 101

7. In view of the amendment filed September 24, 2007, the Examiner withdraws the rejection of claims 15-28 under 35 U.S.C. 101.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. Claims 1-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Meltzer "Vulnerability Detection Systems (VDS) FAQ", pages 1-13, January 2003 in view of Bunker, V et al. US 2003/0056116 (hereinafter Bunker).

2. As per claims 1, 3, 15-16 and 29-30:

3. Meltzer teaches a system for real-time vulnerability assessment of a host/device, said system comprising: an agent running on the host/device, said agent comprising: a first data structure for storing the status of interfaces and ports on the interfaces of the host/device, an executable agent module coupled to the first data structure to track the status of interfaces and ports on the interfaces of the host/device and to store the information, as entries in said first data structure, said executable agent module to compare the entries to determine a change in the status of interfaces and/or of ports on the interfaces of the host/device, (page 5, 1.6 How does a VDS protect my network? , pages 6-12, 2. How do Vulnerability Detection Systems Work?)

a remote destination server, said destination server comprising, a second data structure

for storing the status of interfaces and the ports on the interfaces of the host/device, an executable server module coupled to the second data structure to receive the information communicated by the agent executable module of the agent on the host/device, said executable server module to store the received information as entries in the second data structure wherein the entries indicate the state of each of the ports on each of the active interfaces of the host/device as received, said executable server module to compare the entries in said data structures to determine the change in the status of interfaces and ports on the interfaces of the host/device, and said executable server module to run vulnerability assessment tests on the host/device in the event of a change in the status of interface/ports. (page 5, 1.6 How does a VDS protect my network? , pages 6-12, 2. How do Vulnerability Detection Systems Work?)

Meltzer does not explicitly teach the nature of the way it reports the vulnerabilities. Bunker in analogous art, however, teaches an interface receives output and translates that output to the command database which is used by the network vulnerability assessment system which combines command engine and a database 114 (that stores the raw data that can be migrated to any data format desired). (page 10, pp. 168-173)

Therefore it would have been obvious to one ordinary skill in the art to modify the method disclosed by Meltzer with Bunker in order to provide a real-time network security vulnerability assessment tests, possibly complete with recommended security solutions. (Abstract; Bunker)

As per claims 2, 4 and 31:

The combination of Meltzer and Bunker teaches all the subject matter as discussed above. In addition, Meltzer further teaches an executable server module coupled to a second data structure to receive and update the vulnerability data in the destination server used by the server for vulnerability tests, whenever new vulnerabilities are discovered, and said executable server module coupled to the second data structure to test the host/device for the new vulnerabilities whenever the vulnerability database is updated with new vulnerabilities and to determine the new vulnerabilities. (page 5, 1.6 How does a VDS protect my network? , pages 6-12, 2. How do Vulnerability Detection Systems Work?)

As per claims 5, 17 and 32:

The combination of Meltzer and Bunker teaches all the subject matter as discussed above. In addition, Bunker further teaches wherein status of an interface is either active or inactive. (page 23, pp. 354)

As per claims 6, 18 and 33:

The combination of Meltzer and Bunker teaches all the subject matter as discussed above. In addition, Bunker further teaches wherein status of a port is a service listening on the port or not. (page 7, pp. 17)

As per claims 7, 19 and 34:

The combination of Meltzer and Bunker teaches all the subject matter as discussed above. In addition, Meltzer further teaches wherein the agent tracks the change in status of ports/interface by monitoring in real-time or polling at periodic intervals for the status of ports/interfaces and storing the entries at various time

intervals. (pages 6-12, 2. How do Vulnerability Detection Systems Work?)

As per claims 8, 20 and 35:

The combination of Meltzer and Bunker teaches all the subject matter as discussed above. In addition, Bunker further teaches wherein the communication protocol between the host/device and the destination server is a standard transport level utility selected from sockets or any other standard communication protocol. (page 10, pp. 168-173)

As per claims 9, 21 and 36:

The combination of Meltzer and Bunker teaches all the subject matter as discussed above. In addition, Meltzer further teaches wherein the server executable module compares the entries corresponding two consecutive time intervals. (pages 6-12, 2. How do Vulnerability Detection Systems Work?)

As per claims 10, 22 and 37:

The combination of Meltzer and Bunker teaches all the subject matter as discussed above. In addition, Meltzer further teaches wherein the host/device is selected from a switch, a router, a device running a standard real-time operating system, a mobile device or a PDA. (pages 6-12, 2. How do Vulnerability Detection Systems Work?)

As per claims 11, 23 and 38:

The combination of Meltzer and Bunker teaches all the subject matter as discussed above. In addition, Meltzer further teaches wherein the host/device is an enterprise/consumer machine running with Windows, Unix, Linux, VxWorks, Symbian or

PalmOS. (pages 6-12, 2. How do Vulnerability Detection Systems Work?)

As per clams 12 and 24:

The combination of Meltzer and Bunker teaches all the subject matter as discussed above. In addition, Bunker further teaches wherein the changes that are communicated to the destination server consisting of the IP address of the interface(s) and the port numbers on which listening services have started or stopped on the particular interface(s). (page 14, pp. 229-page 16, pp. 263)

As per claims 13 and 25:

The combination of Meltzer and Bunker teaches all the subject matter as discussed above. In addition, Bunker further teaches wherein the status of the port consists of separate statuses for TC and UD protocols. (page 14, pp. 229-page 16, pp. 263)

As per claims 14 and 26-28:

The combination of Meltzer and Bunker teaches all the subject matter as discussed above. In addition, Bunker further teaches wherein plurality of hosts/devices is tracked in conjunction with one or more destination servers handling the host/devices. (page 14, pp. 229-page 16, pp. 263)

4. Claims 1, 3, 15-16 and 29-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf et al. us 6,324,656 (hereinafter Gleichauf) in view of Barnett "NOOSE-Networked Object-Oriented Security Examiner", USENIX 2000, pages 369-378.

As per claims 1, 3, 15-16 and 29-30:

Gleichauf teaches a system for real-time vulnerability assessment of a host/device, said system comprising: an agent running on the host/device, (figure 2, item 20) said agent comprising: a first data structure for storing the status of interfaces and ports on the interfaces of the host/device, an executable agent module coupled to the first data structure to track the status of interfaces and ports on the interfaces of the host/device and to store the information, as entries in said first data structure, said executable agent module to compare the entries to determine a change in the status of interfaces and/or of ports on the interfaces of the host/device, (col. 3, line 42-col. 4, line 67; col. 5, lines 27-col. 6, line 31)

a remote destination server, (figure 2, item 40) said destination server comprising, a second data structure for storing the status of interfaces and the ports on the interfaces of the host/device, an executable server module coupled to the second data structure to receive the information communicated by the agent executable module of the agent on the host/device, said executable server module to store the received information as entries in the second data structure wherein the entries indicate the state of each of the ports on each of the active interfaces of the host/device as received, said executable server module to compare the entries in said data structures to determine the change in the status of interfaces and ports on the interfaces of the host/device, and said executable server module to run vulnerability assessment tests on the host/device in the event of a change in the status of interface/ports. (col. 3, line 42-col. 4, line 67; col. 5, lines 27-col. 6, line 31)

Gleichauf does not explicitly teach the nature of the way it reports the vulnerabilities. Barnett in analogous art, however teaches a framework for the implementation of vulnerability management system using agents, which reside on particular hosts, to gather information that are then transferred to the NOOSE architecture, and the NOOSE architecture has the means to store host specific configuration and vulnerability data. (page 371, figure 2; page 370, col. 2, pp. 2, page 374, col. 2, pp.3) Therefore it would have been obvious to one ordinary skill in the art to modify the method disclosed by Gleichauf with Barnett in order to have a system that presents the vulnerability information as an integrated database. (Abstract; Barnett)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shewaye Gelagay whose telephone number is 571-272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Shewaye Gelagay SG

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER